(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 00151901 B1

(43)Date of publication of application: 24.06.1998

(21)Application number: 95039935

(22)Date of filing: 06.11.1995

(51)Int. Cl H04L 9/32

(71)Applicant: SK TELECOM CO., LTD.

(72)Inventor: LEE, JONG BONG
YOU, JI WON

(54) METHOD FOR AUTHENTICATING MOBILE TERMINAL USING SECRET NUMBER

(57) Abstract:

PURPOSE: A method for authenticating a mobile terminal using a secret number is provided to prevent an illegal reproduction by using a secret number between a mobile terminal and a switching system.

CONSTITUTION: A method for authenticating a mobile terminal using a secret number comprises the steps of a comparison process, a transmission process, a decision process, and an ending

process. The comparison process is to compare a secret number received from a mobile terminal with a secret number stored in a switching system. The transmission process is to transmit an increased value for the secret number to the mobile terminal. The decision process is to change the secret number in the mobile terminal and determine the reception status. The ending process is to change the secret number in the switching system or finish the process.

Legal Status

Date of request for an examination (19951106)

Final disposal of an application (registration)

Date of final disposal of an application (19980617)

Patent registration number (1001519010000)

Date of registration (19980624)

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl. [6]
H04L 9/32

(11) 공고번호 특0151901
(24) 등록일자 1998년06월24일

(21) 출원번호	특1995-039935	(65) 공개번호	특1997-031533
(22) 출원일자	1995년11월06일	(43) 공개일자	1997년06월26일

(73) 특허권자 에스케이텔레콤주식회사 서정욱
서울특별시 중구 남대문로 5가 267 남산그린빌딩

(72) 발명자 유지원
대전시 유성구 전민동 삼성푸른아파트 112동 1402호
이종봉
대전시 유성구 전민동 청구나래아파트 103동 1306호

(74) 대리인 박해천

심사관 : 임영희

(54) 비밀 번호를 이용한 이동 단말기 인증 방법

요약

본 발명은 비밀번호를 이용한 이동 단말기의 인증 방법에 관한 것으로, 본 발명의 수행을 위한 프로그램을 저장하는 ROM(30)과 비밀번호를 쓰고 읽기 위한 소거/기록이 가능한 EEPROM(50)을 포함하는 인증 장치의 비밀번호(AFKN)를 이용한 이동 단말기의 인증 방법에 있어서, 단말기로부터 비밀번호를 수신하여 교환기에 저장된 비밀번호와 상기 단말기로부터 수신된 비밀번호의 값을 비교하는 제1단계(100 내지 102); 상기 제1단계(100 내지 102)에서 동일하면 음성채널 할당시 상기 단말기로 비밀번호에 대한 증가치(DAFKN)를 송신하고, 동일하지 않으면 상기 단말기로부터 수신된 AFKNm 값이 교환기에 저장된 AFKNs 값에 DAFKN를 합한 값과 동일한지를 비교하여 동일하면 교환기의 비밀번호(AFKNs)를 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값으로 변경한후 음성채널 할당시 상기 단말기로 DAFKN을 송신하는 제2단계(103 내지 106); 상기 단말기는 교환기로부터 수신된 DAFKN의 값과 AFKNm의 값을 합하여 비밀번호를 변경한 후 SAT를 리턴하고, 교환기는 음성채널 연결확인 신호가 수신되었는지 판단하는 제3단계(107); 및 상기 제3단계(107)에서 음성채널 연결 확인 신호가 수신되면 교환기의 비밀번호(AFKNs)에 증가분(DAFKN)을 합하여 교환기의 비밀번호를 변경한후 새로운 DAFKN을 설정하고, 음성채널 연결확인 신호가 수신되지 않았으면 기존의 AFKNs 값과 DAFKN의 값을 저장하고 종료하는 제4단계(108 내지 110)를 포함하여 이동 단말기와 교환기의 비밀번호를 매 통화시 변경하므로 설령 공간 전파 도청을 통해 복제를 하더라도 가입자가 이를 인지하여 대처할 수 있으며, 또한 자기복제의 경우에도 오직 하나의 단말기만 사용할 수 있어 불법복제를 방지할 수 있는 효과가 있다.

명세서

[발명의 명칭]

비밀 번호(AFKN)를 이용한 이동 단말기 인증 방법

[도면의 간단한 설명]

제1도는 본 발명이 적용되는 시스템 구성도.

제2도는 본 발명의 일실시예에 따른 발신시의 처리 흐름도.

제3도는 본 발명의 일실시예에 따른 착신시의 처리 흐름도.

제4도는 본 발명의 다른 실시예에 따른 전체 흐름도.

* 도면의 주요부분에 대한 부호의 설명

10 : 중앙 처리 장치(CPU) 20 : 디코더

30 : 롬(ROM) 40 : 램(RAM)

50 : 이이피롬(EEPROM)

[발명의 상세한 설명]

본 발명은 비밀 번호를 이용한 이동 단말기의 인증 방법에 관한 것이다. 이동 단말기가 급속도로 보급되면서 이동 단말기에 대한 불법 복제가 성행하고 있다. 이동 단말기의 불법복제한 하나의 이동 단말기에 고유하게 부여되는 전화번호(Mobile station Identification Number, 이하 'MIN'이라 함), 장치 일련 번호(Electronic Serial Number, 이하 'esn'이라 함)를 다른 단말기에 복제하는 것을 말하며, 이렇게 하여 한 가입자가 두개 이상의 이동 단말기를 사용하거나 또는 타인의 번호를 도용하여 사용하는 경우를 말한다.

이러한 불법복제를 방지하기 위하여 종래에는 교환시스템의 데이타를 실시간 수집 분석 검증하여 불법 가입자를 찾아내는 방법과 기지국 마다 'Phone print'라는 RF 장치를 설치하여 가입자 단말기의 RF 특징을 이용하여 불법 가입자를 찾아내는 방법을 사용하였다. 또한 고유 번호를 추가하여 불법복제를 막는 방법으로 PIN(Personal ID Number) 번호를 사용하는 방법이 있는데, 이 방법은 가입자가 전화를 사용할 때 타인의 불법복제는 막을 수 있으나, 자기복제나 공간 전파를 도청하여 복제하는 것은 막을 수 없을뿐만 아니라 가입자가 전화를 사용할 때 PIN 번호를 다이얼링 해야 하므로 사용이 불편한 문제점이 있었다.

상기한 같은 종래 기술의 문제점을 해결하기 위하여 안출된 본 발명은 이동 단말기의 불법복제를 막기 위하여 비밀 번호를 이용하여 교환기와 이동 단말기간 상호 인증하게 하므로서 불법복제를 막을수 있는 비밀 번호를 이용한 이동 단말기의 인증 방법을 제공하는데 그 목적이 있다.

상기 목적을 달성하기 위한 본 발명은 본 발명의 수행을 위한 프로그램을 저장하는 ROM과 비밀번호를 쓰고 읽기 위한 소거/기록이 가능한 EEPROM을 포함하는 인증 장치의 비밀번호(AFKN)를 이용한 이동 단말기의 인증 방법에 있어서, 단말기로부터 비밀번호(AFKNm)를 수신하여 교환기에 저장된 비밀번호(AFKNs)와 상기 단말기로부터 수신된 비밀번호(AFKNm)의 값을 비교하는 제1단계, 상기 제1단계에서 AFKNs와 AFKNm의 값이 동일하면 음성 채널 할당시 상기 단말기로 비밀번호(AFKN)에 대한 증가치(DAFKN)를 송신하고, AFKNs와 AFKNm의 값이 동일하지 않으면 상기 단말기로부터 수신된 AFKNm 값이 교환기에 저장된 AFKNs 값에 증가치(DAFKN)를 합한 값과 동일한지를 비교하여 동일하지 않으면 호처리를 중지하고, 동일하면 교환기의 비밀번호(AFKNs)를 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값으로 변경한 후 음성채널 할당시 상기 단말기로 DAFKN을 송신하는 제2단계, 상기 단말기는 수신된 DAFKN의 값과 AFKNm의 값을 합하여 비밀번호를 변경한 후 SAT(Supervisory Audio Tone)를 리턴하고, 교환기는 음성채널 연결확인 신호가 수신되었는지 판단하는 제3단계, 상기 제3단계에서 음성채널 연결확인 신호가 수신되면 교환기의 비밀번호(AFKNs)에 증가분(DAFKN)을 합하여 교환기의 비밀번호를 변경한후 새로운 DAFKN을 설정하고, 음성채널 연결확인 신호가 수신되지 않았으면 기존의 AFKNs 값과 DAFKN의 값을 저장하고 종료하는 제4단계를 포함하는 것을 특징으로 한다.

또한, 상기 목적을 달성하기 위한 다른 실시예의 본 발명은 본 발명의 수행을 위한 프로그램을 저장하는 ROM과 비밀번호를 쓰고 읽기 위한 소거/기록이 가능한 EEPROM을 포함하는 인증 장치의 비밀번호(AFKN)를 이용한 이동 단말기의 인증 방법에 있어서, 단말기로부터 비밀번호(AFKNm)를 수신하여 교환기에 저장된 비밀번호(AFKNs)와 상기 단말기로부터 수신된 비밀번호(AFKNm)의 값을 비교하는 제1단계; 상기 제1단계에서 AFKNs와 AFKNm의 값이 동일하면 음성 채널 할당시 상기 단말기로 새로운 비밀번호(AFKN)를 송신하고, AFKNs와 AFKNm의 값이 동일하지 않으면 상기 단말기로부터 수신된 AFKNm 값이 교환기에 저장된 이전의 비밀번호(AFKNs) 값과 동일한지를 비교하여 동일하지 않으면 호처리를 중지하고, 동일하면 교환기의 비밀번호(AFKNs)를 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값으로 변경한 후 음성채널 할당시 상기 단말기로 새로운 AFKN을 송신하는 제2단계; 상기 단말기는 교환기로부터 수신된 새로운 AFKN의 값으로 비밀번호를 변경한 후 SAT를 리턴하고, 교환기는 음성채널 연결 확인 신호가 수신되었는지 판단하는 제3단계; 및 상기 제3단계에서 음성채널 연결 확인 신호가 수신되면 교환기의 비밀번호(AFKNs)를 새로운 비밀번호로 변경한 후 새로운 비밀번호(AFKN)를 설정하고, 음성채널 연결 확인 신호가 수신되지 않았으면 기존의 AFKNs 값과 새로운 AFKN의 값을 저장하고 종료하는 제4단계를 포함하는 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 일실시예를 상세히 설명한다.

제1도는 본 발명이 적용되는 시스템의 구성도로서, 도면에서 10은 중앙 처리 장치(CPU), 20은 디코더(Decoder), 30은 롬(ROM), 40은 램(RAM), 50은 EEPROM(Eletrically Erasable and Programable Read Only Memory)을 각각 나타낸다.

ROM(30)에는 본 발명을 수행하기 위한 프로그램과 ESN이 저장되며, 중앙 처리 장치(10)는 상기 ROM(30)의 데이타를 읽어 본 발명을 수행한다. RAM(40)은 일반적인 데이타를 읽고 쓰기 위한 메모리이고, 소거/기록이 가능한 EEPROM(50)에는 본 발명에 필요한 가변 비밀 번호가 쓰여지고 읽혀진다. 본 발명을 수행하기 위한 이동 단말기와 교환기의 하드웨어 구성은 서로 유사하다.

이동 전화 서비스에 가입한 가입자가 처음 단말기를 사용하면 이동 단말기의 EEPROM(50)에 저장된 가입자가 알지 못하는 임의의 비밀번호 AFKN(Anti Fraud Key Number)가 송신되어 교환기의 메모리 수단에 저장된다. 이후 단말기를 사용하면 저장된 AFKN의 값을 이용해 인증 과정을 수행한다. 또한 교환기는 AFKN에 대한 증가치 DAFKN(Delta AFKN)을 단말기로 전송하여 단말기의 EEPROM(50)에 저장된 AFKN의 값과 교환기에 저장된 AFKN의 값을 수시로 변경할 수 있다.

제2도는 본 발명의 일실시예에 따른 발신시의 처리 흐름도를 나타낸다.

먼저 발신 단말기로부터 MIN, ESN, 상대방 전화번호(Dialied Digits) 및 상기 단말기에 저장된 비밀번호(AFKNm)을 수신하여(100) MIN과 ESN을 이용하여 상기 단말기의 사용가능 여부를 확인한다(101). 상기 단말기에 대한 확인 확인 작업이 완료되면 교환기에 저장되어 있던 비밀 번호(AFKNs)와 상기 단말기로부터 수신한 비밀 번호(AFKNm)의 값을 비교하여 동일한지를 판단한다(102). 비교결과 동일하면 음성 채널 할당시 상기 단말기로 비밀번호(AFKN)에 대한 증가분(DAFKN)을 송신한다(103). 비교 결과 동일하지 않으면 상기 단말기로부터 수신된 비밀번호(AFKNm) 값이 교환기에 저장된 비밀번호(AFKNs)에 증가분(DAFKN)을 합한 값과 동일한지를 비교하여(104) 동일하지 않으면 호처리를 중지하고(105), 동일하면 상기 단말기로부터 수신된 비밀번호(AFKNm) 값으로 교환기의 비밀번호(AFKNs) 값을 대치하고(106), 음성채널을 할당하면서 상기 단말기로 비밀번호의 증가분(DAFKN)을 송신한다(103). 여기서 교환기에 저장된 비밀번호(AFKNs)와 상기 단말기로부터 수신된 비밀번호(AFKNm)를 비교하여 일치하지 않을 경우 교환기에 저장된 AFKNs 값에 증가분(DAFKN)을 합하여 검증 단계를 더 수행하는 이유는 교환기에서 단말기로 증가분(DAFKN)을 송신하였지만 단말기가 수신하지 못하였거나, 또는 단말기는 수신하고, 단말기가 음성채널로 SAT(Supervisory Audio Tone) 리턴 신호를 송신하였지만 교환기가 음성채널 연결확인 신호를 수신하지 못한 경우를 대비한 것이다. 상기 단말기는 교환기로부터 증가분(DAFKN)을 수신하면 상기 단말기에 저장된 비밀번호(AFKNm)에 증가분(DAFKN)을 합하여 저장하고, 할당된 음성채널을 통해 SAT를 단말기로 보내면 단말기는 SAT를 리턴한다. 교환기는 음성채널 연결확인 신호를 수신하면(107) 교환기에 저장된 비밀번호(AFKNs)에 증가분(DAFKN)을 합하여 비밀번호를 변경하여 저장하고(108), 다음에 사용할 DAFKN을 새로이 설정한다(109). 교환기는 음성채널 연결확인 신호를 수신하지 못하면 기존의 AFKNs값과 DAFKN값을 그대로 유지한다(110).

제3도는 본 발명의 일실시예에 따른 착신시의 처리 흐름도를 나타낸다.

착신시는 착신 단말기로부터 페이지(PAGE)에 대한 응답시 MIN, ESN 및 비밀번호(AFKN)를 함께 수신하면(200), MIN과 ESN을 이용하여 상기 단말기의 사용가능 여부를 확인한다(201). 이후의 과정은 발신시의 과정과 동일하므로 여기서는 약하기로 한다.

제4도는 본 발명의 또다른 실시예에 따른 전체 흐름도를 나타낸다.

이동 단말기로부터 MIN, ESN 및 상기 단말기에 저장된 비밀번호(AFKNm)을 수신하면(300) MIN과 ESN을 이용하여 상기 단말기의 사용가능 여부를 확인한다(301). 상기 단말기에 대한 확인 작업이 완료되면 교환기에 저장되어 있던 비밀번호(AFKNs)와 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값을 비교하여 동일한지를 판단한다(302). 비교 결과 동일하면 음성 채널 할당시 상기 단말기로 새로운 비밀번호(AFKN)를 송신한다(303). 비교 결과 동일하지 않으면 상기 단말기로부터 수신된 비밀번호(AFKNm) 값이 교환기에 저장된 이전의 비밀번호(AFKNs) 값과 동일한지를 비교하여(304) 동일하지 않으면 호처리를 중지하고(305), 동일하면 상기 단말기로부터 수신된 비밀번호(AFKNm) 값으로 교환기의 비밀번호(AFKNs) 값을 대치하고(306), 음성채널을 할당하면서 상기 단말기로 새로운 비밀번호(AFKN)를 송신한다(303). 상기 단말기는 교환기로부터 새로운 비밀번호(AFKN)를 수신하면 상기 단말기에 저장된 비밀번호(AFKNm)에 새로운 비밀번호(AFKN)로 변경하고, 할당된 음성채널을 통해 SAT를 단말기로 보내면 단말기는 SAT를 리턴한다. 교환기는 음성채널 연결확인 신호를 수신하면(307) 교환기에 저장된 비밀번호(AFKNs)를 새로운 비밀번호로 변경하고(308), 다음에 사용할 새로운 비밀번호(AFKN)를 설정한다(309). 교환기는 음성 채널 연결확인 신호를 수신하지 못하면 기존의 AFKNs 값과 새로운 AFKN 값을 저장한다(310).

상기와 같이 구성되어 동작하는 본 발명은 이동 단말기와 교환기의 비밀번호를 매 통화시 변경하므로 설령 공간 전파 도청을 통해 복제를 하더라도 가입자가 이를 인지하여 대처할 수 있으며, 또한 교환기에서 가입자의 통화 내역을 기록할 때 매 통화시의 비밀번호를 기록하면, 가입자 단말기에 저장된 비밀번호를 읽어 교환기에서 기록한 비밀번호 내역과 비교하므로서 어느 통화부터 도용당했는지를 확인할 수 있다. 또한 자기복제의 경우에도 오직 하

나의 단말기만 사용한 수 있어 불법복제를 방지할 수 있는 효과가 있다.

(57)청구의 범위

청구항1

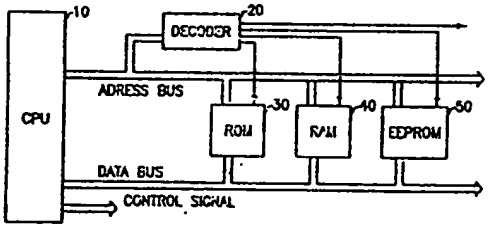
본 발명의 수행을 위한 프로그램을 저장하는 ROM(30)과 비밀번호를 쓰고 읽기 위한 소거/기록이 가능한 EEPROM(50)을 포함하는 인증 장치의 비밀번호(AFKN)를 이용한 이동 단말기의 인증 방법에 있어서, 단말기로부터 비밀번호(AFKNm)를 수신하여 교환기에 저장된 비밀번호(AFKNs)와 상기 단말기로부터 수신된 비밀번호(AFKNm)의 값을 비교하는 제1단계(101 내지 102); 상기 제1단계(100 내지 102)에서 AFKNs와 AFKNm의 값이 동일하면 음성채널 할당시 상기 단말기로 비밀번호(AFKN)에 대한 증가치(DAFKN)를 송신하고, AFKNs와 AFKNm의 값이 동일하지 않으면 상기 단말기로부터 수신된 AFKNm 값이 교환기에 저장된 AFKNs 값에 증가치(DAFKN)를 합한 값과 동일한지를 비교하여 동일하지 않으면 호처리를 중지하고, 동일하면 교환기의 비밀번호(AFKNs)를 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값으로 변경한 후 음성채널 할당시 상기 단말기로 DAFKN을 송신하는 제2단계(103 내지 106); 상기 단말기는 수신된 교환기로부터 수신된 DAFKN의 값과 AFKNm의 값을 합하여 비밀번호를 변경한 후 SAT를 리턴하고, 교환기는 음성채널 연결확인 신호가 수신되었는지 판단하는 제3단계(107); 및 상기 제3단계(107)에서 음성채널 연결확인 신호가 수신되면 교환기의 비밀번호(AFKNs)에 증가분(DAFKN)을 합하여 교환기의 비밀번호를 변경한후 새로운 DAFKN을 설정하고, 음성채널 연결확인 신호가 수신되지 않았으면 기존의 AFKNs 값과 DAFKN의 값을 저장하고 종료하는 제4단계(108 내지 110)를 포함하는 것을 특징으로 하는 비밀번호를 이용한 이동 단말기의 인증 방법.

청구항2

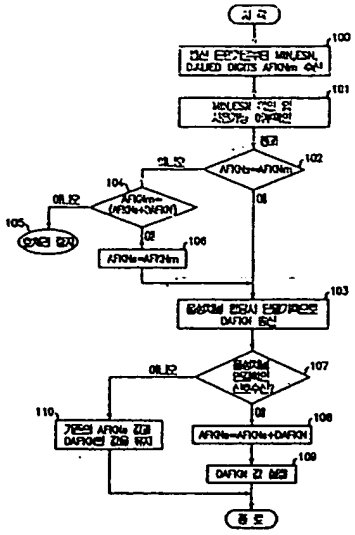
본 발명의 수행을 위한 프로그램을 저장하는 ROM(30)과 비밀번호를 쓰고 읽기 위한 소거/기록이 가능한 EEPROM(50)을 포함하는 인증 장치의 비밀번호(AFKN)를 이용한 이동 단말기의 인증 방법에 있어서, 단말기로부터 비밀번호(AFKNm)를 수신하여 교환기에 저장된 비밀번호(AFKNs)와 상기 단말기로부터 수신된 비밀번호(AFKNm)의 값을 비교하는 제1단계(300 내지 302); 상기 제1단계(300 내지 302)에서 AFKNs와 AFKNm의 값이 동일하면 음성채널 할당시 상기 단말기로 새로운 비밀번호(AFKN)를 송신하고, AFKNs와 AFKNm의 값이 동일하지 않으면 상기 단말기로부터 수신된 AFKNm 값이 교환기에 저장된 이전의 비밀번호(AFKNs) 값과 동일한지를 비교하여 동일하지 않으면 호처리를 중지하고, 동일하면 교환기의 비밀번호(AFKNs)를 상기 단말기로부터 수신한 비밀번호(AFKNm)의 값으로 변경한 후 음성채널 할당시 상기 단말기로 새로운 AFKN을 송신하는 제2단계(303 내지 306); 상기 단말기는 교환기로부터 수신된 새로운 AFKN의 값으로 비밀번호를 변경한 후 SAT를 리턴하고, 교환기는 음성채널 연결확인 신호가 수신되었는지 판단하는 제3단계(307); 및 상기 제3단계(307)에서 음성채널 연결확인 신호가 수신되면 교환기의 비밀번호(AFKNs)를 새로운 비밀번호로 변경한 후 새로운 비밀번호(AFKN)를 설정하고, 음성채널 연결확인 신호가 수신되지 않았으면 기존의 AFKNs 값과 새로운 AFKN의 값을 저장하고 종료하는 제4단계(308 내지 310)를 포함하는 것을 특징으로 하는 비밀번호를 이용한 이동 단말기의 인증 방법.

도면

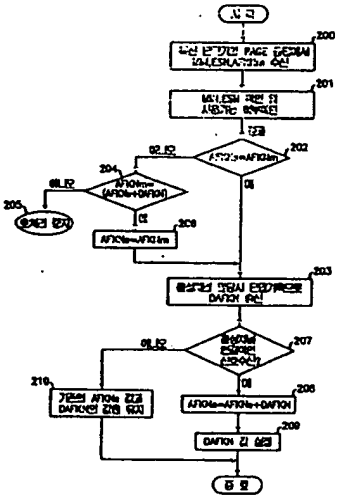
도면1



도면2



도면3



도면4